No. 25-1411

IN THE
United States Court of Appeals for the Fourth Circuit

AMERICAN FEDERATION OF STATE, COUNTY AND MUNICIPAL EMPLOYEES, AFL-CIO, et al.,

Plaintiffs-Appellees,

v.

SOCIAL SECURITY ADMINISTRATION, et al.,

Defendants-Appellants.

On Appeal from the U.S. District Court
for the District of Maryland
Case No. 1:25-cv-00596

BRIEF OF PLAINTIFFS-APPELLEES

BRIAN A. SUTHERLAND
ANNA-ROSE MATHIESON
Complex Appellate Litigation Group LLP
96 Jessie Street
San Francisco, CA 94105

ALETHEA ANNE SWIFT
MARK B. SAMBURG
EMMA R. LEIBOWITZ
SIMON C. BREWER
ROBIN F. THURSTON
Democracy Forward Foundation
P.O. Box 34553
Washington, DC 20043
(202) 448-9090

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

INTRODUCTION

The Social Security Administration is entrusted with vast quantities of sensitive, personally identifiable information. Beyond just Social Security numbers, it maintains systems of records that include medical and mental health information, family court and children's school records, and other highly sensitive information. The Agency is obligated by the Privacy Act and its own regulations, practices, and procedures to keep that information secure—and not to share it beyond the circle of those who truly need it. Since its founding, SSA has been committed to living up to its data security obligations. But in a sudden and striking departure from generations of precedent, the Agency now seeks to throw open its data systems to non-Agency employees who lack standard training on handling personally identifiable information ("PII"), completed background investigations, or demonstrated need for the PII they seek.

To protect Plaintiffs' members from irreparable harm during proceedings taking place at "breakneck speed," Dist. Ct. Doc. 162 at 1, the district court entered a limited preliminary injunction to preserve the *status quo ante* and to safeguard Plaintiffs' members' private

information, JA1293. The district court supported that injunction with a 148-page opinion, supplying extensive findings of fact and demonstrating that its interim relief was both narrow in scope and necessary to protect Plaintiffs from irreparable harm while the legality of the Agency's actions was further assessed. *See generally* JA1299–1446. This Court, sitting en banc, declined to stay the district court's injunction, although the Supreme Court subsequently granted an application to stay the injunction pending resolution of the appellate process.

This Court should affirm. Plaintiffs suffer a cognizable injury caused by Defendants' abandonment of long-settled safeguards securing the public's most sensitive data, and they have demonstrated a strong likelihood of success on the merits. Defendants' actions were final, and they flout established legal standards and longstanding agency policy. And the district court's injunction is properly tailored to remedying the acute effects of Defendants' violations of the law.

STATEMENT OF JURISDICTION

The district court exercised jurisdiction over this case under 28 U.S.C. § 1331. JA1303 n.3. After that court entered a preliminary

injunction, JA1293, Defendants filed a timely notice of appeal, JA1447. This Court therefore has jurisdiction under 28 U.S.C. § 1292.

STATEMENT OF THE ISSUES

This appeal presents the following questions:

(1) Whether the district court erred in concluding that:

a. Plaintiffs have standing to seek injunctive relief when the government grants access to their members' most private information, including financial and health records, in violation of the Privacy Act, Agency regulations, and longstanding policy and procedure; or

b. Defendants violated the Privacy Act by providing unfettered access to agency systems of records containing the PII of millions to individuals with no demonstrated need to access that PII.

(2) Whether the district court erred in concluding that:

a. Defendants' adoption of a new policy of access to systems of records, which constituted a "sea change" in agency policy, was a final agency action reviewable under the Administrative Procedure Act; or

b. Defendants' decision to provide individuals with expansive access to SSA record systems without signed detail agreements, adequate training, completed background investigations, executive work forms, and/or actual need and without (1) acknowledging that they were departing from standard agency practices, (2) considering the reliance interests of Plaintiffs and millions of others with information at the Agency, or (3) considering the risks posed by such access was arbitrary and capricious in violation of the APA.

(3) Whether the district court properly exercised its discretion in finding that:

a. Plaintiffs' members will be irreparably harmed by Defendants' provision of their most sensitive, confidential, and personally identifying information to DOGE Team members without signed detail agreements, adequate training, completed background investigations, executive work forms, and/or actual need;

b. A limited injunction will not irreparably harm the government; and

c. The public interest favors an injunction pausing SSA's policy change.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and regulations are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

I. SSA'S COLLECTION, MAINTENANCE, AND PROTECTION OF DATA

SSA was established in 1935 and is now the government's largest benefits-paying agency. JA1302, JA1306. In addition to overseeing essential programs, including Old-Age, Survivors, and Disability Insurance ("Social Security") and Supplemental Security Income ("SSI"), it helps administer programs run by other agencies, including Medicare, Medicaid, and SNAP. JA1313.

To effectuate its own and other agencies' programs, SSA collects and stores some of the most sensitive information a person may have. Along with Social Security numbers, names, birth dates, and addresses—already sensitive information often used by malicious actors to commit serious fraud—SSA records include, among other things, employment and wage histories; financial data, including tax return information and

bank account and credit card numbers; marriage certificates; school records; family court records; citizenship, immigration, and naturalization records; and medical records documenting information such as evaluations, hospitalizations, treatment, diagnoses, and disabilities, whether they relate to physical or mental health. JA1314.

Since the Agency's founding, SSA has understood the importance of protecting the confidentiality of this sensitive, personal information. The first regulation SSA published included a "commitment to the public to safeguard the personal information [people] entrust" to SSA. JA1443; 2 Fed. Reg. 1256 (June 18, 1937). Even today, the Agency's website advertises that SSA maintains "the highest level of privacy protections possible." *SSA's Commitment to Protecting Privacy through Compliance*, Soc. Sec. Admin., https://perma.cc/779M-XJ7H; JA1443 (citing *id.*). Based on these and other facts, the district court concluded that the Agency has an "entrenched, longstanding policy and practice" of "guarding the confidentiality and privacy of PII, except as needed, and, when needed, allowing only tailored access." JA1392.

That includes "the policy of 'least privilege,' by which 'a user [is] given no more privileges than those necessary to perform their job.'" *Id.*

(quoting the Administrative Record). The Agency emphasizes the importance of least-privilege access in part because "[u]nlimited rights and access can equate to unlimited potential for damage," and "[t]he more privileges an account or user has, the greater potential for abuse or errors." JA1393 (same). SSA's Information Security Policy thus "instructs managers to '[r]estrict access to information systems to the minimum level required to perform assigned duties'" and to "ensure adequate 'separation of duties' within the roles of Information Systems." JA1393–1394 (same). Also referred to as "segregation" of duties, separation of duties "'is the idea that no user should have enough privileges to misuse a system on their own.'" JA1395 (quoting a declaration by former SSA Chief Information Officer Marcela Escobar-Alava, JA506).

II. THE PRIVACY ACT OF 1974

SSA is also bound by the Privacy Act of 1974, which restricts the use and disclosure of data both within and outside the Agency. Congress enacted the Act, 5 U.S.C. § 552a, "to protect the privacy of individuals identified in information systems maintained by Federal agencies." *Doe v. Chao*, 540 U.S. 614, 618 (2004) (quoting Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896). The statute was spurred by "rightful

and broad condemnation of government surveillance programs including Watergate and the FBI's COINTELPRO," *Garris v. FBI*, 937 F.3d 1284, 1295 (9th Cir. 2019), and its passage reflected Congress's recognition that "[t]he increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from" the government's handling of Americans' sensitive information, Pub. L. No. 93-579, § 2(a)(2).

To protect against those risks, the Privacy Act regulates federal agencies' "collection, maintenance, use, and dissemination of" such data. Pub. L. No. 93-579, § 2(a)(5). As relevant here, the Act prohibits agencies from disclosing covered data except in certain enumerated circumstances, such as where agency employees "have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1).

III. EXECUTIVE ORDER NO. 14,158

On January 20, 2025, President Trump issued an executive order creating the "Department of Government Efficiency" and setting forth its agenda: "modernizing [f]ederal technology and software to maximize governmental efficiency and productivity." Exec. Order No. 14,158 § 1, 90

Fed. Reg. 8441 (Jan. 20, 2025) (the "E.O."). The E.O. renamed the United States Digital Service the "United States DOGE Service (USDS)" and reorganized it within the Executive Office of the President. *Id.* § 3(a). Plaintiffs refer to USDS and the U.S. DOGE Service Temporary Organization collectively as "DOGE."

The E.O. directed the heads of every federal agency to establish a "DOGE Team," whose leaders would be selected "in consultation with" the USDS Administrator and who would "coordinate their [teams'] work with USDS." *Id.* § 3(c). Agency heads were also instructed to "take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems." *Id.* § 4(b); *see also id.* § 4(a). Like most executive orders, the E.O. states that it "shall be implemented consistent with applicable law." *Id.* § 5(b); *id.* § 5(a)(i).

IV. DOGE AT SSA

DOGE began its work at SSA on January 30, 2025, demanding immediate access to all systems, data, and source code but failing to articulate a need for such expansive access. JA1324–1325. Sensitive to

the requirements of the Privacy Act and the Agency's own regulations, practices, and policies, Agency leadership offered to provide anonymized and read-only data that would enable DOGE to pursue its work without exposing PII. JA1325. The resulting standoff led to the resignation of top SSA officials who had refused to provide data access on DOGE's terms. JA1325–1326.

Leland Dudek, an SSA employee who had been put on leave for unauthorized data sharing, was designated acting commissioner. Ken Thomas, *The Newly Elevated Acting Head of Social Security Covertly Helped DOGE*, Wall Street J. (Feb 20, 2025), https://perma.cc/F3V3-XG9R. SSA then granted the DOGE Team unfettered access to Agency data systems containing enormous quantities of sensitive, private, and personally identifiable records. JA1302; *see also* JA1303 (quoting counsel for the government's acknowledgment that SSA had "provide[d] DOGE affiliates with access to a 'massive amount' of records"). Doing so ran counter to longstanding regulations and agency policies regarding the principles of least-privilege access and segregation of duties, which explicitly reflect the Agency's understandings of its obligations under the Privacy Act. JA1392–1399, JA1415 (citing JA1601).

V. PRIOR PROCEEDINGS AND RELATED CASE

Plaintiffs are two national labor and membership associations and one grassroots advocacy organization with a combined membership of around 7.6 million. Those members are harmed by DOGE's unlawful records access at SSA, which one described as "almost like someone breaking into [her] house and stealing stuff." JA1362 (quoting JA491). Plaintiffs therefore filed suit against SSA and related defendants on February 21, 2025,[1] and amended their complaint to reflect the rapidly changing facts on March 7. JA19. Plaintiffs simultaneously moved for a temporary restraining order, supporting their motion with ten declarations, including one from former SSA senior executive Tiffany Flick, who was acting chief of staff to the acting commissioner when DOGE arrived at the Agency. JA51–112; JA267–287.

After a lengthy hearing, *see* JA132–235, the district court issued a TRO supported by a 137-page opinion, JA236–378. The TRO barred the disclosure of PII to DOGE personnel at the Agency under certain

[1] Plaintiffs sue on behalf of their members, and the district court correctly concluded that they could do so. JA1383.

circumstances and, *inter alia*, required the same personnel to disgorge and delete any PII previously obtained. JA236–241.

Mere hours later, then-Acting Commissioner Dudek threatened to cease Agency operations. JA379. The district court directed the government to contact chambers if it had any concerns about the text of the Order or needed clarification thereof. JA379–381. The government did not. Instead, it appealed the TRO to this Court, where a panel dismissed the appeal for lack of appellate jurisdiction. *See* No. 25-1291, Doc. No. 20 (Apr. 1, 2025).

The government consented to 14-day extension of the TRO to allow for briefing on Plaintiffs' motion for a preliminary injunction. JA409. That motion supplemented the record with eleven additional declarations, including those of former Agency leadership and experts on agency systems and data security. JA477–515. Defendants produced an administrative record but did not submit any declarations in connection with their opposition to the preliminary injunction. *See* JA517. And while the district court indicated that it would be "helpful" for Acting Commissioner Dudek to appear at the motion hearing to address the various SSA projects "for which he claim[ed] the DOGE team required

access to PII," the government elected to "stand on the record in its current form," JA1182, JA1310.

The district court issued a preliminary injunction on April 17. JA1293–1298. The injunction was accompanied by a 148-page memorandum opinion that addressed the "extensive evidence" in the case, "refin[ed] the pertinent legal analysis" from the court's prior opinion, and addressed *AFT v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025), another case challenging DOGE access to PII in agency systems of record. Dkt. 20, at 1–15 (King, J., concurring) (reviewing the injunction and memorandum opinion).

The district court found that Defendants had not established a need for the unfettered access they sought to grant DOGE Team members, as is required by the Privacy Act's "need to know" exception to the general ban on disclosure. JA1432–1433 (describing the Agency's explanations of need as "imprecise, contradictory, and insufficient"); *id.* JA1435–1436 ("[T]he mere utterance of the word 'need' is not like the proverbial 'get out of jail free card.'"). It also found that Defendants had run "roughshod over SSA protocols for proper hiring, onboarding, training, and, most important, access limitations and separation of duties." JA1435–1436.

The court therefore concluded that Plaintiffs are likely to succeed on their claims that Defendants' conduct violated the Privacy Act and Administrative Procedure Act. *Id.*

The court also determined that the invasion of Plaintiffs' members' privacy could not be rectified after final judgment, in part because SSA maintains uniquely sensitive PII, including records reflecting individual diagnoses of health conditions like HIV and STDs. It also concluded, *inter alia*, that Defendants' sudden desire to pursue anti-fraud projects the Agency had been considering for years but had not "gotten around to" was insufficient to establish that the government would suffer irreparable harm absent a stay. JA1443 (quoting statements by Acting Commissioner Dudek to the district court). And the district court concluded that, despite the government's valid interests in "rooting out possible fraud, waste, and mismanagement," the public interest favored an injunction preventing the "intrusion into the personal affairs of millions," especially in light of SSA's long history of privacy protection and the fact that its systems contain particularly sensitive medical records and financial information. JA1442–1443.

The same day the injunction issued, the government appealed and moved for a stay pending appeal from the district court; it filed a motion for a stay with this Court the following day. JA17. The district court denied that application on April 22, and this Court—sitting en banc—did the same on April 30. *Id.*; *see generally* Dkt. 20. The government then sought a stay pending appeal from the Supreme Court, which was granted on June 6 in a per curiam order. *SSA v. AFSCME*, 145 S. Ct. 1626 (2025). That stay will remain in place pending disposition of this appeal and any subsequent petition for a writ of certiorari. *Id.* Although the Supreme Court recited the factors courts must consider when deciding whether to grant a stay, it did not address how those factors apply to the facts of this case or which factor prompted the stay. *Id.* Moreover, the order explicitly contemplates that this Court may rule otherwise and that the Supreme Court may deny review. *Id.* And the Supreme Court's grant of a stay is not always indicative of its disposition on the merits. *See, e.g.*, *Allen v. Milligan*, 599 U.S. 1, 10 (2023) (reflecting the Court's stay of an injunction and subsequent affirmance of the same on the merits); *Biden v. Texas*, 597 U.S. 785, 794–95, 814 (2022)

(reflecting the Court's denial of a stay but subsequent reversal of the same judgment and injunction).

SUMMARY OF ARGUMENT

Based on a thorough review of the record and relevant case law, the district court correctly granted a preliminary injunction. As the district court found, Plaintiffs suffer an Article III injury-in-fact from ongoing access to their highly sensitive personal information stored at SSA. Improper access to that information inflicts a harm similar to the one long recognized as the tort of intrusion upon seclusion. And SSA's modification of its data-access policy to allow the DOGE Team access to the PII of millions of Americans qualifies as a final agency action reviewable under the APA.

On the merits, Plaintiffs are likely to show that Defendants' conduct is unlawful. The Privacy Act imposes substantive limits on agencies' data-sharing, and Defendants fail to show that any statutory exception authorizes the access granted to the DOGE Team. Even if they could, the agency's decision to modify the data-access policy was arbitrary and capricious because it failed to articulate the reasons for its decision,

consider alternatives, or weigh Plaintiffs' members' serious reliance interests.

The remaining equitable factors favor Plaintiffs, as the district court concluded. Plaintiffs' privacy interests would be irreparably harmed absent an injunction, and the balance of equities tips sharply in Plaintiffs' favor. That is particularly true because the injunction is properly tailored to remedying the acute effects of Defendants' violations of the law while facilitating the DOGE Team's continued work at the Agency. It permits access to redacted or anonymized information when the persons to whom access is given have completed customary training, background checks, and paperwork. Further, it allows access to "discrete, particularized, and non-anonymized" information when the Agency obtains a written statement from the relevant DOGE Team member explaining the need for the record and why anonymization is not feasible. That condition reflects the requirements of the Privacy Act, SSA regulations, and longstanding Agency practice and policy.

STANDARD OF REVIEW

"The purpose of a preliminary injunction is merely to preserve the relative positions of the parties until a trial on the merits can be

held." *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013). Whether to issue or deny a preliminary injunction is committed to the district court's discretion. This Court will not disturb its decision "unless the record shows an abuse of that discretion" regardless of whether this Court would have decided the matter differently in the first instance. *Centro Tepeyac v. Montgomery Cnty.*, 722 F.3d 184, 188 (4th Cir. 2013) (en banc) (citation modified).

ARGUMENT

I. THE DISTRICT COURT CORRECTLY CONCLUDED THAT IT HAD JURISDICTION

The government challenges the district court's determinations that Plaintiffs' members suffer an Article III injury-in-fact caused by Defendants' conduct and that said conduct was a final agency action. Def. Br. 9–10.[2] Neither argument has merit.

1. Plaintiffs Have Standing

The district court correctly concluded that Defendants' actions are causing Plaintiffs injury-in-fact. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (explaining that injury-in-fact is the first of Article III's

[2] Cites to Defendants' opening brief are to the electronic pagination, which does not always correspond to the document's native numbering.

standing requirements and requires "'an invasion of a legally protected interest' which is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"); *United States v. Sells Eng'g*, 463 U.S. 418, 422 n.6 (1983) (concluding that the government's continued unauthorized access to a person's private information, here in the context of a DOJ subpoena of grand jury material, was an ongoing and redressable harm).

Defendants' primary argument on this point is that Plaintiffs "assert a purely intangible form of injury" that amounts to a "bare statutory violation." Def. Br. 32–33. But a "tangible" harm is not necessary to satisfy Article III's concreteness requirement. Intangible harms are sufficiently "concrete" if they bear "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021) (citation omitted). A statutory violation may therefore give rise to standing based on "a close historical or common-law analogue for the[] asserted injury" for which courts have "traditionally" provided a remedy. *TransUnion*, 594 U.S. at 424 (citing, *inter alia*, *Gadelhak v. AT&T Servs.*,

Inc., 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.)). Here, that common-law analogue is the tort of intrusion upon seclusion.

A. *TransUnion* expressly identified intrusion upon seclusion as a tort traditionally recognized as providing a basis for lawsuits in American courts. *Id.* at 425. Intrusion upon seclusion is rooted in the common law right to privacy, the broad contours of which were outlined by Samuel Warren and Louis Brandeis in 1890. Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). Warren and Brandeis defined the right to privacy as the right "to be let alone" and emphasized that privacy violations involve an "injury to the feelings." *Id.* at 195, 197. William Prosser further developed modern privacy law, including by describing the invasion of privacy as "not one tort, but a complex of four." William L. Prosser, *Privacy*, 48 Calif. L. Rev. 382, 389 (1960). Prosser defined the four versions as:

> (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
> (2) public disclosure of embarrassing private facts about the plaintiff;
> (3) publicity which places the plaintiff in a false light in the public eye; and
> (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

JA1354 (citing *id.*). Those four torts "are tied together by the common name [i.e., invasion of privacy], but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff . . . 'to be let alone.'" Prosser, 48 Calif. L. Rev. at 389 (citation omitted); *contra* Def. Br. 53 (emphasizing public disclosure despite its irrelevance to intrusion upon seclusion). The Restatement (Second) of Torts adopts Prosser's understanding of intrusion upon seclusion, as have many states and the District of Columbia. *Restatement (Second) of Torts* § 652B (Am. Law. Inst. 1977); JA1354–1356 (collecting cases).

The Restatement defines the tort as: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement § 652B; *see* Eli A. Meltz, *No Harm, No Foul: Attempted Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 Fordham L. Rev. 3431, 3440–41 (May 2015) (most states have explicitly adopted the Restatement's formulation or one closely mirroring it).

B. Physical ingress is not required. Intrusion upon seclusion may occur by an "investigation or examination into [the plaintiff's] private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents." Restatement § 652B cmt. b; Restatement § 652B (intrusion upon seclusion occurs where someone "intentionally intrudes, physically *or otherwise*, upon the solitude or seclusion of another *or his private affairs or concerns*" if the intrusion "would be highly offensive to a reasonable person" (emphasis added)).

Supreme Court jurisprudence recognizes the same principles: An intrusion into the privacy of *personal information* may constitute a tort of intrusion upon seclusion, even if no spatial barrier is broken. *See, e.g.*, *DOJ v. Reps. Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of *information* concerning his or her person." (emphasis added)). So does this Court. *See, e.g.*, *O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 245 n.2 (4th Cir. 2023) (defining intrusion

upon seclusion as a cause of action "'against defendants who invade[] the private solitude of another'" (quoting *Gadelhak*, 950 F.3d at 462)).

Intrusion upon seclusion does not require the use or disclosure of the confidential information obtained. *See, e.g.*, Restatement § 652B cmt. b; *Nayab v. Cap. One Bank (USA), N.A.*, 942 F.3d 480, 492 (9th Cir. 2019); *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 286 (2d Cir. 2023); *Persinger v. Sw. Credit Sys., LP*, 20 F.4th 1184, 1193 (7th Cir. 2021); *AFL-CIO v. Dep't of Lab.*, No. 1:25-cv-339, 2025 WL 1129227, at *6 (D.D.C. Apr. 16, 2025) (Bates, J.). Disclosure or publication are elements of other torts, such as disclosure of private information, but those are irrelevant here. *TransUnion*, 594 U.S. at 425 (listing disclosure of private information and intrusion upon seclusion separately); *O'Leary*, 60 F.4th at 245–46 (addressing those torts independently).

Likewise, this Court has never found that individual "targeting" is necessary for finding an analog to intrusion upon seclusion, and the evidentiary record makes clear that Plaintiffs' injuries are distinct from hacks or leaks of "various databases that are millions upon millions of rows long." *Cf. Bessent*, 2025 WL 1023638, at *5 (Richardson, J., concurring). And courts have rejected that principle in similar

contexts. *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601–06 (9th Cir. 2020) (finding that allegations about surreptitious data collection stated a claim for intrusion upon seclusion under California law). Even if that were not the case, Defendants have not been shy about the DOGE Team's efforts to review individual records—and even contact the individuals whose PII they improperly accessed. *See, e.g.*, JA399 (stating that two DOGE Team members were "working on individual cases" and might be "reaching out to individuals in connection with those cases").

C. The district court properly concluded, based on extensive legal analysis and fact-finding, that the harm Plaintiffs suffer is sufficiently analogous to that worked by intrusion upon seclusion. JA1346–1383. Defendants' arguments to the contrary rely on misreadings of *O'Leary*, 60 F.4th 240; *Krakauer v. Dish Network, LLC*, 925 F.3d 643 (4th Cir. 2019); and *Garey v. Farrin*, 35 F. 4th 917 (4th Cir. 2022). *See* Def. Br. 42–48.

First, Defendants liken Plaintiffs' claims to the alleged in injury in *O'Leary*, which "lacked the defining feature of the common-law tort." Def. Br. 44. That accurately describes the standing defect in *O'Leary*, but the

holding is inapplicable here. JA1357–1362. The *O'Leary* plaintiff alleged injury caused by his decision to "hand over his partial SSN in exchange for finding out whether he was impacted by [a] data breach," and the Court found his claims not actionable because he alleged only an "abstract privacy interest in his SSN itself." 60 F.4th at 245–46. In this case, the intrusion into private affairs is much more sweeping. *See* JA1361.

Defendants' conduct involves "far more than access to even complete SSNs. It involves access to a wide swath of confidential and sensitive PII, such as medical and mental health records, financial and bank information, tax records, work histories, birth certificates, and personal records concerning children." JA1361. Moreover, Plaintiffs allege more than an "abstract privacy interest." In sworn testimony, members of each Plaintiff organization expressed "unease" caused by DOGE's unfettered access to this information—exactly what the *Bessent* stay panel deemed essential to an intrusion upon seclusion claim. *See Bessent*, 2025 WL 1023638, at *4 (Richardson, J., concurring); JA491 ("DOGE having access to my sensitive information is almost like someone breaking into my house and stealing stuff."); JA69, JA73, JA99,

(expressing similar feelings of "anxiety," "distress," and invasion of "privacy and person").

Second, Defendants overread *Garey* and *Krakauer* to require interjection into a plaintiff's home. *See* Def. Br. 43 (emphasizing that the unwanted telemarketing calls in *Krakauer* were made "to the individual's residence" and that the improper advertisements in *Garey* were "mailed to the individual's home"). They do not.

In *Garey*, this Court found that plaintiffs had standing to sue for an alleged violation of a federal statute providing a cause of action when a person "knowingly obtains, discloses or uses personal information, from a motor vehicle record,' for an impermissible purpose." *Garey*, 35 F.4th at 920 (citing 18 U.S.C. § 2724(a)). The defendants obtained motor vehicle accident reports from state law enforcement agencies or "private data brokers" that contained names and home addresses of the drivers. *Id.* at 919–20. They then used that personal information "to mail unsolicited attorney advertising materials to the drivers involved in those crashes." *Id.* at 920.

The *Garey* panel concluded that the plaintiffs had alleged "a legally cognizable privacy injury." *Id.* at 922. The panel reasoned that the alleged

harm was "closely related to the invasion of privacy, which has long provided a basis for recovery at common law." *Id.* at 921–22 (citation modified). In doing so, it cited this Court's recent opinion in *Krakauer*, 925 F.3d at 643, which *Garey* said involved a "nearly identical standing challenge." *Garey*, 35 F.4th at 921. *Krakauer* was a class action lawsuit involving violations of the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227, which, *inter alia*, prohibits calls to residential phone numbers on the national "Do-Not-Call" registry and provides a private right of action for violations of the statute. 925 F.3d at 648. *Krakauer* analogized the harm in that case, unwanted phone calls to the home, to that associated with the tort of intrusion upon seclusion. *Id.* at 653.

It is well settled that "intrusion upon seclusion can occur beyond the confines of the home," and "the government overreaches when arguing for such a limited understanding of the tort." *Bessent*, 2025 WL 1023638, at *5. As other federal courts of appeals have explained, it is private *affairs* that are protected by the tort, not private s*paces*. *Dickson v. Direct Energy, LP*, 69 F.4th 338, 345 (6th Cir. 2023) (noting that the "kind of harm vindicated by the intrusion-upon-seclusion tort is relatively broad"); *see, e.g.*, *Fletcher v. Price Chopper Foods of Trumann,*

Inc., 220 F.3d 871, 877 (8th Cir. 2000). The government's argument that Plaintiffs have not alleged analogous injury in fact because there was no invasion of their physical space is wrong.

Based on this record evidence and its correct understanding of the tort of intrusion upon seclusion, the district court properly found that the unrestricted access to PII that SSA provided to the DOGE Team would be highly offensive to an objectively reasonable person. JA1382. As the court explained: "If receiving a single unwanted text message or phone call is sufficiently offensive to constitute concrete harm for standing purposes, in the context of intrusion upon seclusion, as several Circuits have determined, then providing the DOGE Team with access to the medical records and sensitive financial information of millions of people, if unauthorized, or without adequate need, is surely sufficiently offensive so as to constitute concrete harm." JA1382.

SSA's records contain the same sensitive information traditionally found and kept in a home ("tax records," "birth certificates"), bank or wallet ("financial and bank information"), physician's office ("medical and mental health records," "hospitalization records"), or other secluded location ("work and earnings history"). JA1314, JA1361. The

government's unauthorized disclosure of that "trove of medical and mental health records," JA1376, would be highly offensive to any reasonable person. In this Circuit, "the disclosure of one's private personnel files and medical records amounts to a per se intrusion into seclusion if the records contain sensitive materials." *Sabrowski v. Albani-Bayeux, Inc.*, 124 F. App'x 159, 161 (4th Cir. 2005) (per curiam) (citation omitted). Other courts throughout the country have concluded the same. *See, e.g.*, *Hooper v. United States*, CL-12-0297, 2013 WL 5530603, at *5 (D. Or. Sept. 25, 2013) ("[A] plaintiff's medical records are considered private, and the unauthorized access or disclosure of the records is an intrusion on seclusion." (citation omitted)); David A. Elder, Privacy Torts §§ 2.6, 2:22 (December 2024 update) (discussing cases in which disclosure of medical or other confidential information amounted to an intrusion on seclusion). The Health Insurance Portability and Accountability Act, 29 U.S.C. § 1181 *et seq.*, and evidentiary psychotherapist-patient privilege further illustrate "the importance of confidentiality" that our society attaches to medical and mental health records. JA1379.

The same is true for detailed, personally identifiable financial information. *See Persinger*, 20 F.4th at 1192 (deeming unauthorized

access to personal financial information analogous to intrusion upon seclusion). Indeed, judge after judge has concluded that DOGE's access to sensitive PII at federal agencies like SSA is "highly offensive." *See, e.g.*, *ARA v. Bessent*, 770 F. Supp. 3d 79, 102–03 (D.D.C. 2025); *AFL-CIO*, 2025 WL 1129227, at *7; *AFGE v. OPM*, 1:25-cv-1237, 2025 WL 996542, at *6 (S.D.N.Y. Apr. 3, 2025).

Congress's enactment of the Privacy Act further underlines this conclusion. *See TransUnion*, 594 U.S. at 425 ("In determining whether a harm is sufficiently concrete . . . Congress's views may be 'instructive.'" (quoting *Spokeo,* 578 U.S. at 341)). Congress can "'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'" *Spokeo*, 578 U.S. at 341 (alteration in original) (quoting *Lujan*, 504 U.S. at 578). And Congress enacted the Privacy Act specifically to "protect the privacy of individuals identified in information systems maintained by Federal agencies." *Doe*, 540 U.S. at 618 (quoting Pub. L. No. 93-579, § 2(a)(5)). As District Judge John Bates recently summarized, Congress "'identified' an individual's interest in his information being viewed only by the federal agency that maintains it—and even then, only by those employees with a need to view it—as 'a

modern relative of a harm with long common law roots.'" *AFL-CIO*, 2025 WL 1129227, at *8 (Bates, J.) (quoting *Gadelhak*, 950 F.3d at 462 (Barrett, J.)); *cf. Carpenter v. United States*, 585 U.S. 296, 392–93 (2018) (Gorsuch, J., dissenting) (discussing, in the Fourth Amendment context, why legislators are well suited to understand privacy concerns).

With respect to agency systems of records, the Privacy Act effectively "created a new sphere in which individuals not only expect privacy, but have a right to it—i.e., a sphere of seclusion." *AFL-CIO*, 2025 WL 1129227, at *8. Intrusion upon that sphere causes injury similar in kind to the intrusion upon other private spheres, such as one's home. *Id.*

That the intruders here are government employees makes no difference. Congress identified a person's interest in their information being viewed "only by those employees with a need to view it." *Id.* (quoting *Gadelhak*, 950 F.3d at 462 (Barrett, J.)), and intrusion upon seclusion pertains to the ability to "choose *when and to what extent* one will permit others to know personal affairs," Theodore R. LeBlang, *Invasion of Privacy: Medical Practice and the Tort of Intrusion*, 18 Washburn L.J. 205, 212 (Winter 1979) (emphasis added). SSA's own regulations reflect the same, defining "disclosure," for purposes of the

Privacy Act, as "making a record about an individual *available* to . . . another party." 20 C.F.R. § 401.25 (emphasis added). "In other words," as the district court explained, "disclosure of a record includes access to the record." JA1412.

The evidentiary record establishes that DOGE Team members have no need for "unbridled access to the [PII] of countless Americans." JA1432. Their intrusion into that sphere of seclusion is sufficient to establish injury in fact. This Court has never required "an exact duplicate in American history and tradition." *TransUnion*, 594 U.S. at 424. Plaintiffs do not need to "import the elements of common law torts, piece by piece," to establish that their members suffer an injury in fact. *See Krakauer*, 925 F.3d at 653. The inquiry is "focused on types of harms protected at common law, not the precise point at which those harms become actionable." *Id.* SSA's decision to disclose to DOGE, without establishing need, "all records of [the Agency,] records that include the highly sensitive personal information of essentially everyone in our Country," Dkt. 20, at 3 (King, J., concurring), inflicts the same type of harm, which is sufficient.

Defendants' argument that Plaintiffs' members cannot show harm because they "voluntarily" shared their PII with the agency ignores that most children are assigned SSNs at birth. It also disregards that Plaintiffs' members *must* share their PII with SSA to access critical benefits that allow them not just to "make ends meet" but also to "survive." *See, e.g.*, JA64, JA70. Even setting that aside, the district court's factfinding establishes that those who "handed over" their sensitive information to SSA had "every reason to believe [it] would be fiercely protected." Dkt. 20, at 6 (King, J., concurring). More generally, disclosure of private information to a third party does not grant that party carte blanche to share it with others. "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts . . . for a limited business purpose need not assume that this information will be released to other persons for other purposes." *Smith v. Maryland*, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (citation omitted).

2. Plaintiffs Challenge a Final Agency Action

SSA's change to its data-access policy dispensed with its 90-year commitment to "the foundational principle of an expectation of privacy

with respect to its records." JA1444. That policy change is a discrete "agency action" within the meaning of 5 U.S.C. § 704.

A. The APA's agency-action requirement should be read "comprehensively" to cover "every manner in which an agency may exercise its power." *Whitman v. Am. Trucking Ass'n*, 531 U.S. 457, 478 (2001) (citation omitted). That is reflected in the statute itself, which specifies that actions "include[] the whole or a part of an agency rule" or "the equivalent" thereof. 5 U.S.C. § 551(13). "Rule" is defined as "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency." *Id.* § 551(4). These definitions make apparent that an agency's decision "to adopt a policy of disclosing confidential information" is an agency action within the meaning of the APA. *Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008); *see also AFL-CIO*, 2025 WL 1129227 at *12 (treating nearly identical access policy changes at other agencies as final agency action and collecting cases).

Defendants principally argue that access decisions as to individual employees do not constitute "agency action" for purposes of the APA. That misapprehends Plaintiffs' claims. As the district court found, Defendants made a discrete decision to change Agency practices, policies, and procedures to allow expansive access to all SSA systems of records—and the PII contained therein—without signed detail or employment agreements, the Agency's prescribed training, completed background investigations, or actual or articulated need. JA1403. Plaintiffs challenge the Agency's adoption of that new access *policy*, a "circumscribed, discrete agency action[]," *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 62 (2004), which is a far cry from an assortment of granular, employee-specific decisions. Reviewing such action is a commonplace and workable role for federal district courts. Agencies may *follow* their access policies "thousands" of times daily, Def. Br. 50, but they adopt or change those policies far less frequently, and reviewing the latter type of action is a far cry from "general judicial review of [agencies'] day-to-day operations," *Lujan v. Nat'l Wildlife Fed.*, 497 U.S. 871, 899 (1990).

B. SSA's decision to adopt wholesale changes to its prior access policies was also "final" under the APA. Agency action is final when it (1)

"mark[s] the 'consummation' of the agency's decisionmaking process," and (2) is "one by which 'rights or obligations have been determined' or from which 'legal consequences will flow.'" *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (citations omitted). The government does not meaningfully contest that the Agency's action meets the first *Bennett* prong, *see, e.g.*, Def. Br. 51, and it plainly satisfies the second as well.

Under the "'pragmatic' approach [the Supreme Court] has long taken to finality," *U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 599 (2016) (citation omitted), SSA's access policy decision "determine[s] the rights of those whose information is being disclosed and the obligations of the [SSA] defendants." *See AFL-CIO*, 2025 WL 1129227 at *13. The Supreme Court has previously recognized that regulations permitting disclosure of information "certainly" affect the individual "confidentiality rights of those who submit [that] information." *Chrysler Corp. v. Brown*, 441 U.S. 281, 303 (1979).

Venetian Casino Resort, 530 F.3d at 925, is informative. In that case, the D.C. Circuit held that an agency's decision to adopt a policy of disclosing confidential information without notice was final agency action for purposes of the APA. *Id.* at 931. In attempting to distinguish *Venetian*

Casino, the government suggests that, in reaching its finality determination, the D.C. Circuit relied on the "immediate material consequences" of third-party disclosure for the plaintiffs in that case. Def. Br. 52–53. But that Court did no such thing. Instead, it held that the agency took final action simply by adopting the "unwritten policy" of disclosing information. *Bhd. of Locomotive Eng'rs & Trainmen v. Fed. R.R. Admin.*, 972 F.3d 83, 100 (D.C. Cir. 2020) (citing *Venetian Casino*). That is because the adoption of the policy itself determined rights and legal obligations with respect to the control and dissemination of the plaintiff's information. *Venetian Casino*, 530 F.3d at 931. It was therefore correct to treat the policy's adoption—not "subsequent activities in carrying it out"—as final agency action. *Vill. of Bald Head Island v. U.S. Army Corps of Eng'rs*, 714 F.3d 186, 195 (4th Cir. 2013).

The other authorities Defendants cite to suggest that third-party disclosure is a necessary component for finality are inapposite. Def. Br. 53. Both *TransUnion* and *Hunstein v. Preferred Collection & Mgm't Servs., Inc.*, 48 F.4th 1236 (11th Cir. 2022) (en banc), concerned whether third-party disclosure was necessary to establish standing on the basis of harm analogous to torts that required third-party disclosure. That

question has no bearing on finality. Moreover, as explained above, intrusion upon seclusion does not require public disclosure.

II. THE DISTRICT COURT CORRECTLY CONCLUDED THAT PLAINTIFFS ARE LIKELY TO PREVAIL ON THE MERITS OF THEIR PRIVACY ACT CLAIM

The district court correctly concluded that Defendants' decision to provide the DOGE Team with expansive access to SSA record systems without actual need violates the Privacy Act.

As discussed above, *see supra* Section II, "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies," the Privacy Act "regulate[s] the collection, maintenance, use, and dissemination of information by such agencies." Pub. L. No. 93-579, § 2(a)(5). Under the Privacy Act, agencies may not "disclose" records except in certain enumerated circumstances, none of which is present here. 5 U.S.C. § 552a(b).

Defendants argue exclusively that SSA's disclosure of Privacy Act records to DOGE Team members is permitted by the "need-to-know" exception of 5 U.S.C. § 552a(b)(1), which allows disclosure of records to employees of the agency "who have a need for the record in the performance of their duties." *Id.* But the district court found, after a

thorough review of the record, that DOGE Team members at SSA do not have a need for the unprecedented and sweeping access they seek. JA1433. Indeed, Defendants made no effort to assess whether DOGE Team members needed the access they received. The justifications they now offer are all post hoc rationalizations, and unpersuasive in any event. Finally, only employees of the agency that controls disclosed records are properly subject to the need-to-know exception, and the members of the SSA DOGE Team are not properly considered employees of SSA.

1. The Privacy Act and "Need to Know"

Defendants have never shown—as they must to avail themselves of the need-to-know exception—that SSA DOGE Team members have a need to access PII contained in SSA's systems of record. On the contrary: the district court's review of the evidence, to which this Court must defer, found that "[t]he Administrative Record does not establish 'need' in any meaningful way," JA1432; that Defendants' proffered explanations are "imprecise, contradictory, and insufficient," *id.*; and that Defendants' "expressed 'need' is amorphous," JA1416.

A careful review of the Administrative Record, SSA regulations, and other record evidence led the district court to conclude that the Privacy Act's "need" requirement should be considered as "need to know." JA1415–1416 ("SSA's policies regarding access decisions appear to be guided by the Agency's understanding of the requirements of the Privacy Act"). SSA's Information Security Policy, for example, instructs as follows:

> Managers authorize access to SSA Information Systems based upon official business "need-to-know," and limited to the "Least Privilege" access required for performing job functions. Whenever access is granted, it is limited access to those who have a legitimate need for these resources to perform their assigned position responsibilities.

JA1393–1394; *see also* JA1758. SSA's regulations provide that employees shall "[d]isclose records within SSA only to an employee who has a *legitimate need to know* the record in the course of his or her official duties." 20 C.F.R. § 401 Add. A (emphasis added). And Tiffany Flick, who worked at SSA for over 30 years and who most recently served as Acting Chief of Staff to Acting SSA Commissioner Michelle King, JA1322, offered unrefuted testimony that the scope of access SSA provides to individual employees requires a "need to know." *See* JA1396 (quoting JA109); JA342. Caselaw reflects the same. JA1416 (interpreting the

"need" requirement and asking "whether the official examined the record in connection with the performance of duties assigned to him" and "had to do so in order to perform those duties properly" (quoting *Doe v. DOJ*, 660 F. Supp. 2d 31, 44–46 (D.D.C. 2009))).

Moreover, the Privacy Act requires the government to show that *each* disclosure was supported by a need. Defendants seek to escape that requirement by advancing a novel theory: that the Privacy Act does not protect information contained within a record so long as an employee has a need for the record itself. Def. Br. 62–63. But that interpretation of the Act misapprehends the nature of "records" and directly contradicts long-standing OMB guidance on implementation of the Privacy Act, which explains that a record is "any item of information about an individual that includes an individual identifier; [i]nclud[ing] any grouping of such information," and "can include as little as one descriptive item about an individual." 40 Fed. Reg. 28949, 28951–52 (July 9, 1975). "A record, by this definition, can include another record." *Id.* at 28952. The relevant statutory question—whether the employee needs access to the PII within a larger record, not whether the employee needs access to the larger

record itself—is the exact opposite question from the one Defendants identify. *See* Def. Br. 62–63.

Defendants' newfound assertion that such a requirement would be unworkable, Def. Br. 63, is a post hoc rationalization belied by record evidence. As Ms. Flick explained in an unrefuted declaration to the district court,

> Normally when analysts or auditors review agency data for possible payment issues, including for fraud, the review process would start with access to high-level, anonymized data based on the least amount of data the analyst or auditor would need to know. If a subset of records within that data are flagged as suspicious, the analyst or auditor would access more granular, non-anonymized data to just that subset of files. In my experience, the type of full, non-anonymized access of individual data on every person who has a social security number or receives benefit[s] from Social Security is unnecessary at the outset of any anti-fraud or other auditing project.

JA1326 (quoting JA126–127). Another unrebutted declaration, from former SSA Chief Information Officer Marcela Escobar-Alava, establishes that "standard practice would be to (1) grant DOGE Team members access to the data they sought in a 'sandbox' environment with anonymized data, and (2) refuse requests for write-access and access to SSA source code." JA1396 (quoting JA506–507).

2. DOGE's Lack of Need-to-Know

The SSA DOGE Team never had, and the government has never identified, a need for unfettered access to any SSA system. Defendants make no effort to so identify one, except with regard to systems accessed in the course of "investigating whether the government has made improper expenditures." Def. Br. 63. Instead, they baldly assert that access to systems is necessarily required for "agency personnel seeking to modernize agency systems." *Id.* at 57. But the government makes no effort to explain why access to Privacy Act-protected information within those systems is needed for those purposes. That is fatal.

Nor does Defendant's one limited articulation of need—"investigating whether the government has made improper expenditures," *id.* at 63—hold up. Defendants have made no effort to address an unrefuted declaration that "when analysts or auditors review agency data for possible payment issues, including for fraud, the review process would start with access to high-level, anonymized data based on the least amount of data the analyst or auditor would need." JA126–127. If indicia of fraud are identified, those analysts or auditors would then, consistent with the Privacy Act, be able to access non-anonymized data

pertaining *only* to suspicious records. *Id.* In other words, even the anti-fraud work the government now characterizes as creating a need for sweeping access in fact only provides a need for access to a limited subset of records, after initial review is conducted on anonymized data. "[F]ull, non-anonymized access of individual data on every person who has a social security number or receives benefits from Social Security is unnecessary at the outset of anti-fraud or other auditing project." *Id.*

Defendants primarily rely on the E.O. to establish their purported need, *see* Def. Br. 56, but executive orders cannot supersede a duly enacted statute and do not demonstrate that any DOGE Team member needs access to any record "in order to perform [his] duties properly." *Bigelow v. Dep't of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000), *cert. denied*, 532 U.S. 971 (2001). While the E.O. purports to provide a reason for the DOGE Teams' work, such generalized direction to the whole of government is not sufficient to meet the Privacy Act's standard that individual agencies determine the need for various individuals to access a given system or record, let alone to permit unfettered access to all systems in that agency. Nor can executive orders, by themselves, "license the defendants to violate the Privacy Act." *Parks v. IRS*, 618 F.2d 677,

681 (10th Cir. 1980). If they could, the president would have license to eliminate Privacy Act protections by fiat. That would frustrate the Privacy Act, which was "designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators and the curiosity of some government administrators." S. Rep. No. 93-1183 (1974).

The district court, after thoroughly reviewing record evidence, determined that Defendants offered only "vague and conclusory assertions" that sweeping access is needed to pursue anti-fraud work. JA1400. Defendants acknowledge that the level of access granted to the SSA DOGE Team was previously granted to only 30 to 40 employees at SSA—less than 0.1% of Agency employees. JA1399. And the district court reviewed each of the alleged explanations upon which Defendants now rely, concluding that "[n]othing in the specific requests suggests that the DOGE Team members required unlimited access to PII to perform their work." JA1427.

At a hearing on Plaintiff's motion for a preliminary injunction, "defense counsel conceded that anonymization of the data is possible, but

contended that it would be burdensome." JA1428. And, with respect to the memorandum Defendants trumpet, Def. Br. 57–58, the district court correctly concluded that the text "does not mean the [DOGE Team's] work cannot be done without PII. Rather, it suggests only that working without PII may cause the work to take longer," JA1427. Defendants now suggest that an agency's determination of the speed at which it wishes to do its work constitutes "need" for Privacy Act purposes, Def. Br. 64. But that argument contradicts established law that the need-to-know exception can only authorize disclosure when the recipient of the information "had to" view the information to do their job. *Bigelow*, 217 F.3d at 877. As the district court explained, "the Privacy Act does not make an exception to permit employees to access PII so that they can improve their speed when a viable alternative is available to them that does not necessitate access to PII." JA1428.

The district court's factual inquiry established that "if need can be found, it is only in defendants' post hoc explanations for 'need,' set forth in Dudek's declarations." JA1428. Even if those declarations could be properly considered part of the record of Agency decision-making—which they cannot, *see infra* note 4—they are contradicted by other evidence.

See, e.g., JA1431 (a sworn declaration from former GSA Technology Transformation Services Director Ann Lewis). They also "fail to make clear why members of the DOGE Team need unfettered access to a wide variety of SSA systems of record that contain personal, sensitive, and private information of millions of Americans." JA1428. Indeed, they often prove the opposite. In a March 27 declaration, for example, Dudek described a "Fraud Detection" project for which data anonymization was not feasible "because it could obscure information useful for identifying fraud." JA1429. But in a supplemental declaration filed the next day, he stated that the DOGE Team member working on the project "plan[ned] to work with non-DOGE Team SSA employees in order to retrieve anonymized, aggregated data." JA1430. Dudek went on to say that the DOGE Team member "need[ed] access to discrete individual data only when anomalies are identified." JA1430. Three days later, he submitted yet another declaration describing his belief that anonymization was not feasible. The district court deemed those contentions "puzzling," given his prior statements, and noted that Dudek neither "shed light on why he changed his position" nor explained why the procedures he previously described were "not workable for the other projects." JA1431. Moreover,

the court noted, "there are several access requests in the Administrative Record that do not seem to fit into the three projects identified by Dudek." JA1430–1431 (comparing those access requests to Dudek's explanations of the DOGE Team's work).

Finally, separate from their position that the DOGE Team's access falls within the need-to-know exception, Defendants note the district court's observation that the need-to-know exception usually applies to a small number of records and suggest that extending that logic would endanger non-DOGE Team SSA employees' access to SSA information. Def. Br. 61. This argument ignores the district court's point: the need-to-know exception generally applies to relatively few records because employees seldom have a need for expansive access to protected information. *See* JA1416–1447 (discussing scale of access in light of limited purposes justifying "need').

3. Lack of Employee Status

The members of the SSA DOGE Team are also not employees of SSA for purposes of the Privacy Act. This, too, independently closes off the need-to-know exception, which "applies only to *intra-agency* disclosures." *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 547 (3d Cir.

1989) (emphasis added). The district court did not reach this issue, instead relying on the factual determination that the DOGE Team had no need for access. JA1416.

To determine which agency, "as a practical matter," employs an individual federal employee, it is appropriate to consider "all the circumstances," including the matters on which an employee works and who supervises them. *Jud. Watch, Inc. v. Dep't of Energy*, 412 F.3d 125, 132 (D.C. Cir. 2005) (citation modified).

The members of the SSA DOGE Team perform DOGE work and are functionally supervised by USDS. Dudek himself confirmed that "DOGE personnel—or, as he called them, 'outsiders who are unfamiliar with nuances of SSA programs'—are calling the shots." JA1322 (citation omitted); JA1391 (quoting Defendants' statement that "the nature of the SSA DOGE Team's composition and projects are in flux" (internal quotation marks and citation omitted)). The government's own characterization of the team's work relies in large part on the E.O., Def. Br. 56–57, which exclusively pertains to work on the DOGE Agenda and provides no indication that DOGE Teams perform work for their host agencies. Indeed, the E.O. requires DOGE Teams to "coordinate their

work with" USDS. To "coordinate" their work with USDS means that the SSA DOGE Team must "bring into a common action, movement, or condition" or "harmonize" their work with USDS. "Coordinate," *Webster's Third New International Dictionary*, 1971. Because *every* agency DOGE Team is subject to the E.O., it would be impossible to read the E.O. as requiring DOGE Teams to be supervised by each agency and simultaneously harmonized in their work. Coordination can therefore only mean that DOGE Teams are required to work in a way that "harmonizes" with the instructions and expectations of USDS. In contrast, those same teams are required only to "advise" agency heads, which requires neither supervision by agency heads nor even any form of alignment with them. In practice, to comply with the E.O., the SSA DOGE Team must be taking direction from and reporting not to the SSA Administrator, but to USDS.[3]

[3] Furthermore, "several employees of the DOGE Team accessed SSA data systems prior to having signed finalized detail agreements from other agencies," and an unrebutted declaration from former SSA senior executive Tiffany Flick establishes that "the agency does not consider a detailee to be an employee of SSA until a detail agreement is signed and finalized." JA1399.

The district court did not abuse its discretion in concluding, on the record before it, that Plaintiffs are likely to succeed on the merits of their claim that SSA's provision to the DOGE Team of expansive access to sensitive PII does not fall within the need-to-know exception to the Privacy Act.

III. THE DISTRICT COURT DID NOT ERR IN FINDING THAT PLAINTIFFS ARE LIKELY TO PREVAIL ON THE MERITS OF THEIR ARBITRARY AND CAPRICIOUS CLAIM

The district court correctly found that Defendants' conduct was arbitrary and capricious in violation of the APA. 5 U.S.C. § 706(2)(A). Defendants' two-paragraph argument provides no rebuttal to that reasoned conclusion. While APA review is deferential, the statute requires that agencies "articulate a satisfactory explanation" for their actions. *Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). Defendants flunk even that minimal standard.

1. Failure to Show Awareness of or Sufficiently Explain Change

An agency must "'display awareness'" that it is changing its position and "'show that there are good reasons for the new policy.'" *Encino Motorcars, LLC v. Navarro*, 579 U.S. 211, 221 (2018) (quoting *FCC v. Fox*

Television Stations, Inc., 556 U.S. 502, 515 (2009)); *accord Jimenez-Cedillo v. Sessions*, 885 F.3d 292, 298 (4th Cir. 2018) (citations omitted). Defendants did neither. As the district court's thorough review of the record shows, Defendants provided no "reasonable explanation for why the entire DOGE Team needs access to the wide swath of data maintained in SSA systems" to effectuate the DOGE agenda at the Agency. JA1435. Nor did they explain why the DOGE Team members who sought unfettered access were not subject to the Agency's standard credentialing and training processes. *See* JA1435–1436. Instead, they "ran roughshod over SSA protocols for proper hiring, onboarding, training, and, most important, access limitations and separation of duties." JA1435–1436.

To support their contention otherwise, Defendants direct the Court to several emails documenting DOGE Team members' requests for data access. *See* Def. Br. 57–61. But those requests—along with the responses they engendered—are insufficient. For example, Defendants highlight then-Chief Information Officer Michael Russo's statement that SSA "investigated options" to protect PII but was unable to find a "solution that enables the necessary analysis to continue at the pace necessary."

Def. Br. 58 (quoting JA546). But that cursory assertion addresses only one of the DOGE Team's many requests for access to PII—not SSA's decision to adopt a new policy permitting unfettered access regardless of sufficient credentialing or actual need. And it explains neither why those alternatives were unworkable nor why the DOGE Team members required such expansive access. Moreover, it is flatly contradicted by a wealth of record evidence. *See, e.g.*, JA1430 (quoting a Dudek declaration, JA455, averring that at least some SSA DOGE work could be accomplished by using "anonymized, aggregated data" and receiving "access to discrete individual data only when anomalies are identified").[4] So is Russo's assertion, elsewhere in the same request, that personnel addressing "improper payments related to data issues" require access not just to three SSA systems of record but also the PII contained therein. JA1423 (citing JA1456). As Tiffany Flick explained in an unrebutted

[4] An agency cannot use declarations or other post hoc rationalizations to provide new reasons supporting its actions. *Dep't of Homeland Sec. v. Regents of the Univ. of California*, 591 U.S. 1, 21 (2020). But here, it is appropriate to consider the declarations for the limited purpose of showing that the agency's contemporaneous reasoning was pretextual. *See Dep't of Com. v. New York*, 588 U.S. 752, 785 (2019) (citing extra-record evidence that "tells a story that does not match the explanation" given).

declaration, "when analysts or auditors review agency data for possible payment issues, including for fraud," the review process begins with "high-level, anonymized data." JA1398–1399 (citing JA126–127).

Other "explanations" are perfunctory. For example, Acting Commissioner Dudek approved a DOGE Team member's request for access to SSA's entire collection of microfiche, which contains untold amounts of PII, based only on his assertion that such access was necessary "to investigate the number of people beyond a reasonable age who can be marked dead." JA1425 (quoting JA1474). Two days later, he granted similarly broad access based only on the requesting individual's statement that he required it "to access identifying information about beneficiaries and their application documents." JA1425 (quoting JA1470). And on March 17, when three DOGE Team members sought access to "SSI claims data," writ large, because they needed such access "to understand how many people request SSI benefits," Acting Commissioner Dudek approved the request without inquiring as to why access to PII could be necessary to determine how many people request benefits. JA1426 (quoting JA1478). Other examples abound. All are broader than Defendants indicate. *Compare* Def. Br. 59 ("Another

request . . . explained that 'select access' to a certain SSA system was needed."), *with* JA561 (the request itself, which seeks "SELECT access to PSSNAP," *and* JA560 (reflecting Dudek's grant of full access to PSSNAP data).

Neither these documents nor other materials in the Administrative Record evidence the Agency's awareness that it was embracing an unprecedented change to longstanding policies and practices governing grants of access to PII. The APA requires more. *See Encino Motorcars,* 579 U.S. at 221.

Moreover, Defendants do not—and cannot—identify anything in the Administrative Record reflecting awareness of (or explanation for) the Agency's abandonment of its requirement that employees have a completed background check before being given access to PII. JA506, JA1400 (evidencing the policy). That requirement has never been perfunctory: as one SSA employee explained, he was not even able to access SSA email systems before completing a full background check at the agency, "much less get access to the Enterprise Data Warehouse," despite already having a fully adjudicated Top Secret-eligible clearance. JA514. But "some of the background investigations for some

DOGE Team members were still pending when they were provided access to PII in the SSA data systems." JA1400 (citing JA124). And "proof of completion of the DOGE Team members' background investigations is a troubling omission from the Administrative Record." *Id.* (citation omitted).

2. Failure to Consider Reliance Interests

Defendants also fail to identify any evidence that Defendants considered Plaintiffs' members' reliance interests or weighed them against competing policy concerns. *See Regents,* 591 U.S. at 30 (requiring that analysis). Nothing in the Administrative Record reflects the Agency's acknowledgment that Plaintiffs' members shared their PII in part because they trusted that it "would be used only to determine whether [they were] eligible for benefits, and not disclosed for any other purpose." JA73, JA1378. Further, the district court highlighted unrebutted evidence that Plaintiffs' members "handed over a lot of information to SSA" on "the promise that they [would] keep it confidential and on the understanding, made clear by the agency's own website, that they value privacy and security." JA1378 (quoting JA483 and other declarations). Defendants ignored those interests completely.

3. Failure to Consider Policy Alternatives

Finally, the record does not reflect Defendants' consideration of important policy alternatives, as the APA requires. *See State Farm*, 463 U.S. at 43, 51. Defendants try to meet their burden by emphasizing the following text:

> We investigated options for masked or otherwise protecting PII-containing [personally identifiable information] and FTI-containing [federal tax information] fields within these records but have not identified a solution that enables the necessary analysis to continue at the pace necessary to respond timely to the fraud and improper-payment-related concerns.

Def. Br. 58 (quoting JA546). First, as discussed above, that text applies to only one request for access. Second, it is unsupported by actual analysis as to why addressing fraud rapidly was necessary or outweighed privacy concerns. And third, is has been disproven by substantial evidence showing otherwise, including statements by the then-Acting Commissioner of the Agency. *See* JA1430 (citations omitted).

Alternatives—including using anonymized data in the first instance and seeking access to fewer systems of record—were clearly "within the ambit of the existing policy," *Regents*, 591 U.S. at 30 (citation modified). That is evidenced not just by SSA's ordinary course of action,

see supra, but also by formal documents reflecting the Agency's policies and procedures, *see, e.g.*, JA1600–1734; JA1819–1974; JA1978–1979.

Defendants contend that this Court should consider the declarations they submitted to the district court when evaluating this point. Def. Br. 59–60. Those documents, while more detailed, are not properly part of this analysis for two reasons. First, while Defendants now describe the declarations as "educat[ional]" materials created for the district judge to help explain the circumstances surrounding the policy change, they previously said the district court "should look at the administrative record itself." *Compare* Def. Br. 60 n.6, *with* JA1237. Second, the declarations are post-hoc rationalizations, which may be considered only in special circumstances not present here. *Dow AgroSciences LLC v. Nat'l Marine Fisheries Serv.*, 707 F.3d 462, 467–68 (4th Cir. 2013) (citations omitted). And the declarations offer "justifications, explanations, and facts" that are wholly absent from or contradict that record, *id.* at 468, and go beyond mere background information or explanation, *see Roe v. Dep't of Def.*, 947 F.3d 207, 221 (4th Cir. 2020), as amended (Jan. 14, 2020). They are relevant only because

they cast doubt on the veracity of Defendants' descriptions of their activities and Agency policy. *See supra* note 4.

In sum, the record reflects only "ambiguous" and "amorphous" explanations of need. JA1436, JA1416. These "thin" justifications, JA1427, are insufficient to satisfy the APA.

4. *Bessent*

Failing to find support in the record, Defendants fall back on a concurrence with the stay panel's decision in *Bessent*. Def. Br. 64–65. There too, their arguments fail.

The concurrence opined that it would not "stretch the imagination" to think, in the abstract, that personnel tasked with modernizing agency systems might need "administrator-level" access to those systems. *Id.* (quoting *Bessent*, 2025 WL 1023638, at *6 (Richardson, J., concurring)). But a reviewing court cannot "supply a reasoned basis for the agency's action that the agency itself has not given." *State Farm*, 463 U.S. at 43 (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 196 (1947)).

Here, Defendants' and DOGE Team members' explanations of need implicate not software and IT modernization but investigations into alleged fraud. *See, e.g.*, JA546, JA561, JA566, JA569, JA570. And record

evidence negates an assumption that IT personnel at SSA have the unfettered access to PII that the DOGE Team sought and obtained. The agency generally does "not provide full access [to] all data systems even to [its] most skilled and highly trained experts." JA108. Write access, which allows users to add, alter, or delete data, is even more restricted. *See* JA511. And IT personnel who "write code to update programmatic systems," including to maintain SSA records, must submit a special request identifying an "emergency business need" and are given access for no longer than 24 hours. *Id.* Indeed, only 30–40 SSA employees—less than 0.1% the Agency's personnel—have access akin to what the DOGE Team requested and obtained. *See* JA127–128 (citations omitted).

The district court correctly determined that Plaintiffs are likely to succeed on the merits of their arbitrary and capricious claim.

IV. THE DISTRICT COURT CORRECTLY DETERMINED THAT PLAINTIFFS ARE LIKELY TO SUFFER IRREPARABLE HARM ABSENT AN INJUNCTION

The district court in no way abused its discretion in finding that Plaintiffs' members are likely to suffer irreparable harm absent an injunction. Rather, it correctly determined that an injunction was

necessary to prevent the government from violating the privacy of Plaintiffs' members without regard for either SSA's well-established practices or other laws, including the Privacy Act.

As the district court found and the government does not contest, the data SSA houses is among the most sensitive information maintained in government systems, and includes "extensive medical and mental health records" and family records. JA1440; *see also* Dkt. 20 at 14 (Heytens, J., concurring) (noting the "scale of information" housed at SSA). Plaintiffs' members turned over their information "with every reason to believe that the information would be fiercely protected." Dkt. 20, at 4, 6 (King, J., concurring). And they cannot be made whole after final judgment: even if Plaintiffs could sue for damages under the limited circumstances permitted by the Privacy Act, *see* 5 U.S.C. § 552a(g)(4), such damages would be both "difficult to ascertain" and "insufficient," *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 551 (4th Cir. 1994) (citation omitted), *abrogated in part on other grounds by Winter v. Nat. Res. Def. Council*, 555 U.S. 7 (2008). In such circumstances, this Court has found injuries to be irreparable. *See id.*; *see also Scrimgeour v. IRS*, 149 F.3d 318, 327 n.11 (4th Cir. 1998).

Moreover, Plaintiffs' members' injuries are not limited to those caused by the DOGE Team's initial improper access to their data. The harm compounds each day the Agency continues to permit individuals without appropriate credentialing or actual need to enjoy unrestricted access to PII. Allowing Defendants to proceed apace without the guardrails set forth in the preliminary injunction—*i.e.*, unlawfully and without regard for either SSA's own well established practices or the privacy interests of millions—perpetuates the privacy harms inflicted on Plaintiffs' members. Defendants' arguments to the contrary are unpersuasive.

First, as detailed above, Defendants' disclosure of Plaintiffs' members' PII to individuals without appropriate credentialing or actual need causes cognizable injury in fact. Because the harms caused by Defendants' conduct are immediate, ongoing, and imminent, they qualify as irreparable injuries. *See Mountain Valley Pipeline, LLC v. 6.56 Acres of Land*, 915 F.3d 197, 216 (4th Cir. 2019).

Second, confidentiality requirements in some DOGE Team members' employment agreements, Def. Br. 66–67, do not preclude a showing of irreparable harm. *See, e.g.*, *Roberts v. Austin*, 632 F.2d 1202,

1205, 1214 (5th Cir. 1980) (holding that plaintiffs suffered irreparable harm where the defendants violated a "statutory protection" against "the disclosure of confidential information," even though the party accessing the information was instructed not to disclose it). Publication may be sufficient to demonstrate irreparable harm. *See, e.g.*, *United States v. Miami Univ.*, 294 F.3d 797, 803, 817–19 (6th Cir. 2002). But the facts of this case—which involves unbounded access to some of the most sensitive and confidential PII maintained in federal systems of record—demonstrate that disclosure without publication can itself inflict irreparable harm.

The Privacy Act itself expressly limits intra-governmental and intra-agency disclosures even though nearly all government employees are bound by confidentiality obligations. That reflects Congress's recognition that harm can result from data access by unauthorized government employees regardless of whether they are bound by confidentiality agreements or disclose the information they obtain. The legislative history of the Act supports the same. "Enacted in the wake of the Watergate and the Counterintelligence Program (COINTELPRO) scandals" the Privacy Act "sought to restore trust in government and to

address what at the time was seen as an existential threat to American democracy." Dep't of Just., *Overview of the Privacy Act: 2020 Edition* (Oct. 4, 2022). Its passage was "designed to prevent" both overzealous investigation and government employees accessing records to satisfy their own curiosity. *See* S. Rep. No. 93-1183 (1974).

Finally, Defendants' reliance on Judge Richardson's *Bessent* stay panel concurrence and three district court decisions, Def. Br. 66–67, is misplaced. Like *Bessent*, those decisions concerned different agencies, different systems of record, and different allegations and evidence. *See generally Univ. of Cal. Student Ass'n v. Carter*, 766 F. Supp. 3d 114 (D.D.C. 2025) (involving DOGE access to student data maintained by the Department of Education); *ARA v. Bessent*, No. 25-cv-313, 2025 WL 740401 (D.D.C. Mar. 7, 2025) (DOGE access to data in systems of record at the Department of Treasury); *EPIC v. U.S. Office of Pers. Mgmt.*, No. 25-cv-255, 2025 WL 580596, at *6–7 (E.D. Va. Feb. 21, 2025) (DOGE access to data in Treasury and OPM systems of record). Unlike the systems at issue in those cases, "SSA records contain extensive medical and mental health records, as well as records involving children." JA1440. And sworn statements establish that "SSA operates one of the

most sensitive data environments in the federal government." JA1168 (noting that the Agency's disability data includes PII on reproductive health). The district court rightly concluded that giving uncredentialed individuals without a need for PII unfettered access to, *inter alia*, highly sensitive and personally identifying medical, school, and family court records inflicts irreparable harm.

While it is "too late" to prevent the invasion of privacy that occurred when DOGE Team members first obtained access to Plaintiffs' members' PII, it is not too late to prevent the ongoing injury to their privacy interests caused by the DOGE Team's continued access. *See Church of Scientology of Cal. v. United States*, 506 U.S. 9, 13 (1992); *In re Grand Jury Investigation No. 78-184*, 642 F.2d 1184, 1187–88 (9th Cir. 1981). That is especially true here, where the district court's injunction "require[d] disgorgement of information" already obtained while "preserving the government's ability to obtain data as needed going forward." Dkt. 20, at 14 (Heytens, J., concurring). The district court correctly found that Plaintiffs' members face irreparable harm from DOGE Team's ongoing access to sensitive systems of record housing their data at the Agency.

V. THE DISTRICT COURT CORRECTLY FOUND THAT THE BALANCE OF EQUITIES AND PUBLIC INTEREST BOTH FAVOR GRANTING AN INJUNCTION

The injunction works no harm on the government and benefits the public interest. The government's two short paragraphs arguing the opposite are telling. Both record evidence and Defendants' briefing reflect "the government's inability to provide a convincing explanation of how it will be tangibly and irreparably harmed" by the injunction. Dkt. 20, at 15 (Heytens, J., concurring).

To start, the injunction is quite narrow: It has no impact on non-DOGE anti-fraud efforts at SSA. It permits the DOGE Team to pursue anti-fraud efforts by allowing Defendants to provide DOGE Team members access to redacted or anonymized data and records once they "have 'received all training that is typically required of individuals granted access to SSA data systems' and have undergone standard background investigations and paperwork," *see* JA1294–1295, in keeping with long-held agency practices, *see* JA1307, JA1400. And it allows SSA to provide DOGE affiliates access to "discrete, particularized, and non-anonymized data" when the Agency complies with the previous requirements and obtains a written explanation from the DOGE Team

member regarding their need for the record, again reflecting the requirements of the Privacy Act and SSA regulations. JA1295.

Nor does the injunction impede the Executive Branch's efforts to modernize the government. The government's reliance on that argument, to be clear, is a new development. The overwhelming majority of Defendants' district-court briefing emphasized anti-fraud initiatives. When asked how DOGE access to sensitive information maintained by the Agency would further its "mission," government counsel responded that the SSA DOGE Team "is broadly charged with looking at fraud at the agency." *See, e.g.*, JA1246–1247. Regardless, the preliminary injunction has no impact on modernization efforts in the same way that it has no impact on anti-fraud efforts: It permits both DOGE and non-DOGE activity at the agency so long as minimal requirements are met.

Likewise, the injunction inflicts no "irreparable constitutional harm" on the President's control over Executive Branch employees or the public's interest in allowing administrations to pursue their policy priorities. *See* Def. Br. 60. The injunction allows the President to pursue the DOGE agenda at SSA. Limited delay may be an inconvenience. But it is certainly not an irreparable harm.

Finally, the public interest favors an injunction. Allowing the President to effectuate his agenda is important, and searching for fraud and waste in the government is, as the district court noted, a "laudable" goal. *See* JA1444. But the public's interest in that direction must be considered alongside the right to individual privacy and the fact that the executive branch must follow the law. Agencies must not "act unlawfully even in pursuit of desirable ends." *Ala. Ass'n of Realtors v. HHS*, 594 U.S. 758, 766 (2021) (per curiam) (citation omitted).

That is especially true here, where Defendants' conduct violates a right that has been protected since the country's founding. *Cf. Carpenter*, 585 U.S. at 304–05. That individual right to privacy is at stake: millions have relied on SSA's commitments to keep their sensitive, personally identifying information confidential for nearly a century. The equities and public interest both support the preliminary injunction.

CONCLUSION

For the foregoing reasons, this Court should affirm the district court's entry of a preliminary injunction.

Respectfully submitted,

ALETHEA ANNE SWIFT
MARK B. SAMBURG
EMMA R. LEIBOWITZ
SIMON C. BREWER
ROBIN F. THURSTON
Democracy Forward Foundation
P.O. Box. 34553
Washington, DC 20043
(202) 448-9090

BRIAN A. SUTHERLAND
ANNA-ROSE MATHIESON
Complex Appellate Litigation Group LLP
96 Jessie Street
San Francisco, CA 94105

July 2025

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 12,993 words. It complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)–(6) because it was prepared using Microsoft Word in Century Schoolbook 14-point font, a proportionally spaced typeface.

/s/ Alethea Anne Swift
Alethea Anne Swift

CERTIFICATE OF SERVICE

I certify that on July 9, 2025, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Service will be accomplished by the appellate CM/ECF system.

/s/ Alethea Anne Swift
Alethea Anne Swift

ADDENDUM

INDEX TO ADDENDUM

5 U.S.C. § 551 – Definitions

For the purpose of this subchapter—

* * *

(4) "rule" means the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency and includes the approval or prescription for the future of rates, wages, corporate or financial structures or reorganizations thereof, prices, facilities, appliances, services or allowances therefor or of valuations, costs, or accounting, or practices bearing on any of the foregoing;

* * *

(13) "agency action" includes the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act; and

5 U.S.C. § 552a – Records maintained on individuals

* * *

(b) Conditions of Disclosure.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality

has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;

(11) to the Director of the Congressional Budget Office, or any authorized representative of the Director, in the course of performance of the duties of the Congressional Budget Office;

(12) pursuant to the order of a court of competent jurisdiction; or

(13) to a consumer reporting agency in accordance with section 3711(e) of title 31.

* * *

(g)

(1) Civil Remedies.—Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

* * *

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

* * *

5 U.S.C. § 704 – Actions reviewable

Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review. A preliminary, procedural, or intermediate agency action or ruling not directly reviewable is subject to review on the review of the final agency action. Except as otherwise expressly required by statute, agency action otherwise final is final for the purposes of this section whether or not there has been presented or determined an application for a declaratory order, for any form of reconsideration, or, unless the agency otherwise requires by rule and provides that the action meanwhile is inoperative, for an appeal to superior agency authority.

5 U.S.C. § 706 – Scope of review

To the extent necessary to decision and when presented, the reviewing court shall decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action. The reviewing court shall—

* * *

(2) hold unlawful and set aside agency action, findings, and conclusions found to be—

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

* * *

20 C.F.R. § 401

§ 401.25 – Terms defined.

* * *

Disclosure means making a record about an individual available to or releasing it to another party.

* * *

Appendix A to Part 401 – Employee Standards of Conduct

(d) Rules governing employees whose duties require use or reference to systems of records. Employees whose official duties require that they refer to, maintain, service, or otherwise deal with systems of records (hereinafter referred to as "Systems Employees") are governed by the general provisions. In addition, extra precautions are required and systems employees are held to higher standards of conduct.

(1) Systems Employees shall:

(a) Be informed with respect to their responsibilities under the Privacy Act;

(b) Be alert to possible misuses of the system and report to their supervisors any potential or actual use of the system which they believe is not in compliance with the Privacy Act and regulation;

(c) Disclose records within SSA only to an employee who has a legitimate need to know the record in the course of his or her official duties;

* * *

40 Fed. Reg. 28949, 28951–52 (July 9, 1975) - Implementation of Section 552a of Title 5 of the United States Code

* * *

Record.—Subsection (a) (4) 'The term 'record' means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, 'and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;"

The term "record", as defined for purposes of the Act, means a tangible or documentary record (as opposed to a record contained in someone's memory) and has a broader meaning than the term commonly has when used in connection with record-keeping systems. (It may also differ from the usual definition of a computer record.) An understanding of the term "record", as it is used in the Act, is essential in interpreting the meaning of many of the Act's requirements.

A "record"

Means any item of information about an individual that includes an individual identifier;

Includes any grouping of such items of information (it should not be confused with the use of the term record in the conventional sense or as used in the automatic data processing (ADP) community);

Does not distinguish between data and information; both are within the scope of the definition; and

Includes individual identifiers in any form including, but not limited to, finger prints, voice prints and photographs.

The phrase "identifying particular" suggests any element of data (name, number) or other descriptor (finger print, voice print,

photographs) which can be used to identify an individual. Identifying particulars are not always unique (i.e., many individuals share the same name) but when they are not unique (e.g., name) they are individually assigned—as distinguished from generic characteristics.

The term "record" was defined "to assure the intent that a record can include as little as one descriptive item about an individual." (Congressional Record, p. 521818, December 17, 1974 and p. H12246, December 18, 1974). This definition "includes the record of present registration, or membership in an organization or activity, or admission to an institution." (Senate Report 93-1183, p. 79). (While this language was written with reference to the definition of the term "personel information" in the Senate bill, it would appear to be equally applicable to the term "record" as used in the Act.)

A record, by this definition, can be Part of another record. Therefore prohibitions on the disclosure of a record, for example, apply not only to the entire record in the conventional sense (such as a record in a computer system), but also to any Rein or grouping of items from a record provided that such grouping includes an individual identifier.

* * *

Exec. Order No. 14,158, 90 Fed. Reg. 8441 (Jan. 20, 2025) –

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. This Executive Order establishes the Department of Government Efficiency to implement the President's DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.

Sec. 2. Definitions. As used in this order:

(a) "Agency" has the meaning given to it in section 551 of title 5, United States Code, except that such term does not include the Executive Office of the President or any components thereof.

(b) "Agency Head" means the highest-ranking official of an agency, such as the Secretary, Administrator, Chairman, or Director, unless otherwise specified in this order.

Sec. 3. DOGE Structure. (a) *Reorganization and Renaming of the United States Digital Service.* The United States Digital Service is hereby publicly renamed as the United States DOGE Service (USDS) and shall be established in the Executive Office of the President.

(b) *Establishment of a Temporary Organization.* There shall be a USDS Administrator established in the Executive Office of the President who shall report to the White House Chief of Staff. There is further established within USDS, in accordance with section 3161 of title 5, United States Code, a temporary organization known as "the U.S. DOGE Service Temporary Organization". The U.S. DOGE Service Temporary Organization shall be headed by the USDS Administrator and shall be dedicated to advancing the President's 18-month DOGE agenda. The U.S. DOGE Service Temporary Organization shall terminate on July 4, 2026. The termination of the U.S. DOGE Service Temporary Organization shall not be interpreted to imply the termination,

attenuation, or amendment of any other authority or provision of this order.

(c) *DOGE Teams.* In consultation with USDS, each Agency Head shall establish within their respective Agencies a DOGE Team of at least four employees, which may include Special Government Employees, hired or assigned within thirty days of the date of this Order. Agency Heads shall select the DOGE Team members in consultation with the USDS Administrator. Each DOGE Team will typically include one DOGE Team Lead, one engineer, one human resources specialist, and one attorney. Agency Heads shall ensure that DOGE Team Leads coordinate their work with USDS and advise their respective Agency Heads on implementing the President 's DOGE Agenda.

Sec. 4. *Modernizing Federal Technology and Software to Maximize Efficiency and Productivity.* (a) The USDS Administrator shall commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems. Among other things, the USDS Administrator shall work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.

(b) Agency Heads shall take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems. USDS shall adhere to rigorous data protection standards.

(c) This Executive Order displaces all prior executive orders and regulations, insofar as they are subject to direct presidential amendment, that might serve as a barrier to providing USDS access to agency records and systems as described above.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,

January 20, 2025.